SCIENCE ZONE INTERNATIONAL CONFERENCE ON LAW, GOVERNANCE AND SOCIAL TRANSFORMATION VOL 2. N.1 2026

QUANTUM SUPREMACY AND THE CRISIS OF KINETIC EQUIVALENCE: REASSESSING "ARMED ATTACK" UNDER THE UN CHARTER

Islombek Abdikhakimov
Head of Artificial Intelligence and Legal Tech Laboratory,
Tashkent State University of Law
islombekabduhakimov@gmail.com

ABSTRACT

The imminent arrival of Cryptographically Relevant Quantum Computers (CRQCs) threatens to render the traditional "kinetic equivalence" framework for cyber warfare obsolete. International law, specifically the jus ad bellum regime enshrined in the UN Charter, has historically relied on physical damage and injury as the primary thresholds for defining an "armed attack" under Article 51. This article argues that the unique capabilities of quantum computing—specifically the ability to retroactively decrypt sensitive state data and instantaneously neutralize critical infrastructure without physical destruction—expose a dangerous lacuna in the current legal definition of the use of force. By analyzing the "Harvest Now, Decrypt Later" (HNDL) strategy through the lens of state responsibility and the law of armed conflict, this study posits that quantum-enabled operations constitute a form of "systemic violence" that may cripple a state's functionality without firing a shot. The article concludes that the international community must move beyond the Schmitt analysis of "scale and effects" to a functionalist interpretation of Article 51, where the irreversible compromise of sovereign cryptographic integrity is recognized as a casus belli.

KEYWORDS

Kinetic Equivalence, Armed Attack, UN Charter, Quantum Supremacy, HNDL, Cyber Warfare, Article 51, Critical Infrastructure

Introduction

The foundational architecture of the United Nations Charter was designed in an era where the use of force was synonymous with physical violence—tanks crossing borders, aerial bombardment, and naval blockades. Article 2(4) prohibits the threat or use of force, while Article 51 preserves the inherent right of individual or collective self-defense only in the event of an "armed attack." For decades, legal scholars and state practitioners have attempted to map these kinetic concepts onto the digital domain, resulting in the doctrine of "kinetic equivalence." This doctrine holds that a cyber operation constitutes an armed attack only if its "scale and effects" are comparable to those of a traditional kinetic assault, typically necessitating physical damage to property or injury to persons (Payne, 2016).

However, the advent of quantum computing destabilizes this analogical framework. As indicated by recent technical assessments, the development of CRQCs will allow adversaries to break the public-key cryptography (such as RSA and ECC) that currently secures the global digital economy and national security apparatuses (Erol, 2025). The threat model known as "Harvest Now, Decrypt Later" (HNDL) implies that state actors are currently exfiltrating vast quantities of encrypted data, waiting for the quantum capability to unlock it (Jena, 2025). This creates a scenario where a state could suffer a catastrophic loss of its strategic secrets, financial integrity, and command-and-control capabilities without a single physical structure being destroyed.

The "quantum reckoning" thus presents a legal paradox: a quantum attack could theoretically dismantle a nation's sovereignty and defensive capacity more effectively than a kinetic invasion, yet fail to trigger the right to self-defense under a strict reading of "kinetic equivalence" (Harkavy, 2025). If the destruction is purely informational—the erasure of trust rather than the erasure of buildings—does it rise to the level of an armed attack? The current legal reliance on physical effects creates a "grey zone" in which adversaries can operate with impunity, inflicting systemic harm that remains just below the threshold of kinetic retaliation (Rajagopalan, 2022).

This article seeks to interrogate the sufficiency of the "scale and effects" test in the quantum era. It examines whether the irreversible compromise of a state's

cryptographic shield should arguably constitute an "armed attack" by virtue of its existential threat to the state's survival. By drawing on the latest scholarship regarding the legal status of data and state responsibility in cyberspace, this study proposes a recalibration of the UN Charter's thresholds to accommodate non-kinetic, yet existentially threatening, quantum operations.

Methodology

This research utilizes a doctrinal legal analysis to assess the compatibility of the "kinetic equivalence" standard with emerging quantum threats. The primary analytical framework involves juxtaposing the text of the UN Charter (specifically Articles 2(4) and 51) against the operational realities of quantum computing as described in recent technical literature. The analysis relies on the "Schmitt Analysis"—a widely accepted set of criteria for assessing cyber operations including severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility—as a baseline for current customary international law (Payne, 2016).

To understand the nature of the "quantum injury," the study incorporates technical reviews of Post-Quantum Cryptography (PQC) and the timelines for CRQC development. This technical grounding is essential for establishing the "immediacy" and "severity" of the threat, which are key components of the legal analysis for self-defense (Erol, 2025). The study specifically examines the HNDL threat model to determine if the pre-positioning of harvested data constitutes a "threat of force" or a preparatory act to an armed attack (Jena, 2025).

Furthermore, the methodology integrates theoretical scholarship on the ontology of digital assets. By analyzing recent arguments on whether computer data qualifies as an "object" under International Humanitarian Law (IHL), the study tests the limits of the "damage to property" requirement in the kinetic equivalence doctrine (Pomson, 2023). This involves a close reading of academic disputes regarding the tangibility of data and whether its alteration or deletion constitutes a use of force comparable to physical destruction.

The research also draws on the law of state responsibility to address the challenge of attribution. Given that Article 51 requires an attack to be attributable to a state to justify self-defense, the study analyzes the "effective

control" standard and its applicability to quantum-enabled cyber operations (Chen et al., 2025). The analysis considers whether the unique signature of a quantum attack—or the lack thereof—complicates the evidentiary burden required for lawful kinetic response.

Finally, the study avoids reliance on unverified internet sources, strictly adhering to the provided academic corpus. This ensures that the legal arguments are grounded in peer-reviewed interpretations of international law and validated technical assessments of the quantum threat landscape.

Results

The analysis yields three primary findings regarding the inadequacy of current legal frameworks. First, the "kinetic equivalence" test, as currently interpreted, fails to capture the systemic risk posed by quantum decryption. Most legal scholars agree that for a cyber operation to constitute an armed attack, it must result in physical destruction or injury (Payne, 2016). A quantum attack that decrypts a nation’s banking system, causing total financial collapse and hyperinflation, results in "effects" that are devastating but non-physical. Under the strict Schmitt analysis, such an event might be categorized as economic coercion or a violation of non-intervention, but not an armed attack justifying kinetic self-defense.

Second, the study finds that the legal status of data is a critical bottleneck for updating the law. If data is not considered a protected "object," its destruction does not technically constitute "damage" under the Law of Armed Conflict (LOAC) (Pomson, 2023). While some scholars argue that the loss of functionality of a computer system constitutes damage, this interpretation is not universally accepted. In a quantum scenario, where data is not destroyed but merely "read" (in the case of espionage) or "manipulated" (in the case of integrity attacks), the argument for "damage" becomes even more tenuous. The results suggest that HNDL operations, which are essentially passive until the moment of decryption, fall into a legal blind spot where they are neither clearly espionage (which is unregulated) nor clearly sabotage (which is prohibited).

Third, the results highlight a "temporal crisis" in the application of Article 51. The right to self-defense is predicated on the occurrence of an armed attack or, under the anticipatory self-defense doctrine (the *Caroline* test), an imminent

threat (Payne, 2016). HNDL decouples the act of intrusion (harvesting) from the act of injury (decryption). By the time the injury occurs—potentially years later when a quantum computer comes online—the "imminence" requirement may have passed, or the attribution trail may have gone cold. The adversary effectively "pre-loads" the injury, making the eventual attack instantaneous and difficult to preempt legally.

The analysis also points to the "attributional void" as a major barrier to the use of Article 51. Attribution in cyberspace is already notoriously difficult due to spoofing and the use of proxies (Chen et al., 2025). A quantum computer could theoretically break encryption keys used for identity verification, allowing an attacker to perfectly impersonate a third party. This capability would make "false flag" operations significantly easier, raising the risk of misattributed retaliation. The high standard of proof required for self-defense—often cited as "clear and convincing evidence"—may be impossible to meet in a post-quantum environment.

Finally, the results indicate that the failure to transition to Post-Quantum Cryptography (PQC) could be viewed as a failure of state responsibility. If a state fails to secure its critical infrastructure against known quantum threats, it may be deemed to have failed in its due diligence obligations, potentially complicating its claim to be the victim of an armed attack (Kastelic, 2019). The "crypto-agility mandate" discussed in technical literature thus transforms into a legal imperative for maintaining the standing to invoke self-defense (Jena, 2025).

Discussion

The "crisis of kinetic equivalence" necessitates a fundamental rethinking of what constitutes violence in the international system. The reliance on physical damage is a relic of the industrial age; in the information age, the integrity of data *is* the integrity of the state. A functionalist approach to Article 51 would argue that any operation which neutralizes the state's ability to perform its core sovereign functions—defense, economic management, public safety—constitutes an armed attack, regardless of whether a building collapses. This "functional equivalence" would align the law with the strategic reality that a quantum decapitation strike is as lethal to a modern state as a nuclear one.

The "Harvest Now, Decrypt Later" strategy further challenges the concept of "peace" in international law. If an adversary is actively harvesting encrypted data with the intent to weaponize it, are they not already engaged in a "use of force" via preparation? The discussion suggests that HNDL should be viewed through the lens of "accumulated events" or "composite acts." Just as a series of minor border skirmishes can cumulatively amount to an armed attack, the systematic harvesting of critical data, combined with the development of offensive quantum capabilities, represents a rolling violation of sovereignty that culminates in an armed attack (Payne, 2016).

However, expanding the definition of armed attack to include non-kinetic quantum operations carries significant risks. It lowers the threshold for the use of kinetic force, potentially leading to escalation. If a state can bomb a data center in response to a data breach, the stability of the international order is threatened. The "rational choice theory" of compliance suggests that states will only adhere to a higher threshold if it serves their interests (Kastelic, 2019). Major cyber powers may prefer a high threshold to retain the freedom to conduct their own cyber operations without fear of kinetic retaliation.

The issue of sovereignty is also central to this reassessment. Recent scholarship argues that the unauthorized entry into a state's cyber infrastructure is a violation of sovereignty, but not necessarily a use of force (Journal of Business, IT, and Social Science, 2017). Quantum computing blurs this line because the "entry" allows for total control. If an adversary holds the quantum keys to a nation's power grid, they exercise "effective control" over that infrastructure. This usurpation of control is arguably a more profound violation of sovereignty than a temporary physical incursion.

The discussion also highlights the role of "due diligence" as a stabilizing norm. If the threshold for armed attack remains high, states must rely on the obligation of due diligence to prevent transboundary harm (Kastelic, 2019). This implies a collective responsibility to monitor and suppress quantum proliferation in the non-state sector. However, due diligence is a standard of conduct, not result; it does not provide a remedy when a state intentionally uses quantum capabilities to harm another.

Ultimately, the discussion points toward the need for a new "interpreting resolution" or a specialized treaty that defines "digital armed attack." Such a definitions would likely hinge on the "scale of effects" on *critical infrastructure functions* rather than physical property. The widespread adoption of PQC is not just a technical fix but a strategic necessity to raise the cost of an attack and preserve the "attributional link" required for legal accountability (Jena, 2025).

Conclusion

The emergence of quantum supremacy creates a fissure in the bedrock of the UN Charter. The doctrine of kinetic equivalence, while useful for bridging the gap between kinetic and cyber warfare in the early internet era, is insufficient for the existential threat posed by quantum decryption. The ability of CRQCs to inflict systemic paralysis without physical destruction exposes the limitations of tying the "use of force" to "damage to objects." HNDL operations currently occupy a legal grey zone, allowing adversaries to undermine the strategic balance under the guise of espionage.

To preserve the relevance of the Charter system, the international community must move toward a functionalist interpretation of Article 51. An "armed attack" in the quantum era must be defined by the severity of its impact on the state's sovereign capacity, not the physical nature of the weapon. This requires recognizing that data integrity is a component of territorial integrity in the digital age. Furthermore, the "imminence" required for self-defense must be re-evaluated to account for the latency of HNDL threats.

Without such a legal evolution, the prohibition on the use of force becomes a "parchment barrier," easily circumvented by adversaries who understand that the most devastating attacks of the 21st century will be silent, instantaneous, and physically bloodless. The crisis of kinetic equivalence is not merely a debate for legal scholars; it is a vulnerability in the collective security architecture of the world.

REFERENCES

Chen, H., Coco, A., Rotondo, A., & Ying, Y. (2025). *The Attribution of Cyber Operations to States in International Law*. Geneva Centre for Security Policy (GCSP).

Erol, V. (2025). The Strategic Imperative of Quantum Readiness: A Comprehensive Review of Post-Quantum Cryptography. *Preprints.org*.

Harkavy, R. (2025). The quantum reckoning: law's next frontier. *International Comparative Legal Guides*.

Jena, J. (2025). The Quantum Security Deadline: Building Crypto-Agility Against 'Harvest Now, Decrypt Later' Threats. *European Journal of Computer Science and Information Technology*, 13(52), 35-52.

Journal of Business, IT, and Social Science. (2017). Cybersecurity and International Law: Defining State Responsibility for Cross-Border Cyberattacks. *Journal of Business, IT, and Social Science*.

Kastelic, A. (2019). *Inducing compliance with international law in cyberspace – State responsibility, countermeasures and the obligations of due diligence*. White Rose eTheses Online.

Payne, T. (2016). Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations. *Lewis & Clark Law Review*, 20(2), 683-715.

Pomson, O. (2023). 'Objects'? The Legal Status of Computer Data under International Humanitarian Law. *Journal of Conflict and Security Law*, 28(2).

Rajagopalan, R. P. (Ed.). (2022). *Future Warfare and Technology: Issues and Strategies*. Observer Research Foundation and Global Policy Journal.

Zafar, A. (2025). Quantum Computing in Finance: Regulatory Readiness, Legal Gaps, and the Future of Secure Tech Innovation. *European Journal of Risk Regulation*, 1–20.